

HONORABLE RONALD B. LEIGHTON

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

**ROADLINK WORKFORCE
SOLUTIONS, L.L.C., a Delaware
Corporation,**

Plaintiff,

VERN MALPASS, an individual.

Defendant.

CASE NO. 3:13-cv-05459-RBL

**ORDER GRANTING
DEFENDANT'S MOTION TO
DISMISS IN PART**

(Dkt. #10)

THIS MATTER is before the Court on Defendant Vern Malpass's Motion to Dismiss #10). Malpass is a former employee of Plaintiff RoadLink Workforce Solutions, L.L.C. Link says Malpass stole customer information and other proprietary resources from his computer before he went to work for a competitor. RoadLink has sued him for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as well as five state law claims.¹

¹ The five state law claims are breach of contract, breach of the implied covenant of good faith and fair dealing, misappropriation of trade secrets, conversion, and breach of the fiduciary duty and the common law duty of loyalty.

1 Malpass seeks dismissal of the two federal claims under Fed. R. Civ. P. 12(b)(6). He
2 argues that, even if RoadLink's allegations are true, his alleged actions do not raise a cause of
3 action under the plain language of either statute. Malpass also argues that if the federal claims
4 are dismissed, this Court does not have subject matter jurisdiction over the remaining claims.
5 Because RoadLink has failed to allege facts that could show that Malpass violated either of the
6 federal statutes, Malpass's Motion to Dismiss the Stored Communication Act and Computer
7 Fraud and Abuse Act claims is GRANTED. However, because the Court retains supplemental
8 jurisdiction (as well as diversity jurisdiction) over the remaining claims, Malpass's Motion to
9 Dismiss the remaining claims for lack of subject matter jurisdiction is DENIED.

10 **I. INTRODUCTION**

11 RoadLink is a warehouse and workforce logistics company. RoadLink provides various
12 services to its clients, including freight handling, warehousing, unloading of merchandise, and
13 other ancillary services such as light maintenance and sanitation. One of RoadLink's largest
14 clients is the Fred Meyer store in Chehalis, Washington. (Dkt. #1, Compl. at ¶10). Defendant
15 Vern Malpass was a RoadLink employee for ten years, until he resigned on April 23, 2013.
16 During that time, Malpass was promoted through the ranks of the company, serving a majority of
17 his tenure as Site Manager at the Chehalis Fred Meyer. As Site Manager, Malpass was
18 responsible for the day-to-day operations and financial management of RoadLink's Chehalis
19 Fred Meyer site, including managing the 250 RoadLink employees at that site. (Dkt. # 1, Compl.
20 at ¶ 12).

21 In order to complete his day-to-day duties as Site Manager, Malpass was issued a
22 computer specifically for the Chehalis Fred Meyer site. On that computer, he maintained and
23 updated RoadLink's Trade Resource files specific to the Chehalis Fred Meyer location, which
24

1 included historical information on hiring needs, communications between RoadLink and the
2 Chehalis Fred Meyer, communications between RoadLink and regional vendors, and other
3 information concerning the operations of the site. Much of the information entered into the
4 computer was stored only on the computer's hard drive, with some communications stored and
5 backed up on the computer's Microsoft Outlook program linked to RoadLink's email system.
6 (Dkt. #1, Compl. at ¶ 13).

7 At the beginning of 2013, Fred Meyer informed RoadLink it would be releasing a request
8 for proposal in order to receive competitive bids for the services that RoadLink was providing at
9 the Chehalis site. (Dkt. #1, Compl. at ¶ 21). Merit Integrated Logistics, one of RoadLink's
10 competitors, sought to obtain at least a portion of the Chehalis Fred Meyer contract. On April
11 23, 2013—after it had already secured a piece of RoadLink's previous contract with the Chehalis
12 Fred Meyer, but before it began performing on that contract—Merit offered Malpass
13 employment as its Site Manager at the Chehalis Fred Meyer. (Dkt. #1, Compl. at ¶ 26). Malpass
14 accepted the offer.

15 As part of his employment with RoadLink, Malpass had signed multiple non-compete,
16 non-solicit, and confidentiality agreements. Nevertheless, before resigning at RoadLink,
17 Malpass copied and permanently deleted Trade Resource files stored on the RoadLink-issued
18 computer for the Chehalis Fred Meyer site.

19 On June 12, 2013, RoadLink filed its complaint against Malpass, alleging multiple state
20 claims and two federal claims relating to his alleged copying and deleting of the Trade Resources
21 files. The two federal claims are based on alleged violations of the Stored Communications Act,
22 18 U.S.C. § 2701, *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*
23
24

1 RoadLink argues that Malpass has hacked and destroyed many RoadLink files that he was not
 2 authorized to access, raising claims under the two federal statutes.

3 Malpass moves to dismiss the federal claims under Fed. R. Civ. P. 12(b)(6). Malpass
 4 argues that his alleged actions do not raise a cause of action under the plain language of the
 5 statutes. Malpass also seeks to dismiss the remaining state law claims under Fed. R. Civ. P.
 6 12(b)(1), arguing that the Court does not have subject matter jurisdiction over them once the
 7 federal claims are dismissed, because the complaint does not allege an amount in controversy
 8 exceeding \$75,000.

9 This position is wrong as a matter of law. The Court has jurisdiction over the case under
 10 28 U.S.C. § 1331 (federal question) and supplemental jurisdiction over the state law claims
 11 under 28 U.S.C. § 1337. Dismissal of the federal claims *might* cause the Court to decline to
 12 exercise its supplemental jurisdiction and to dismiss the claims under § 1337(c)(3)—unless, as is
 13 the case, the Court also has original diversity jurisdiction over the claims under 28 U.S.C. §1331.
 14 In no event, however, is it true that the court does not have subject matter jurisdiction over the
 15 claims asserted in Plaintiffs complaint.

16 II. DISCUSSION

17 A. Standard of Review

18 Dismissal under Fed. R. Civ. P. 12(b)(6) may be based on either the lack of a cognizable
 19 legal theory or the absence of sufficient facts alleged under a cognizable legal theory. *Balistreri*
 20 v. *Pacifica Police Dep’t*, 901 F.2d 696, 699 (9th Cir. 1990). A complaint must allege facts to
 21 state a claim for relief that is plausible on its face. *See Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.
 22 Ct. 1937, 1949 (2009). A claim has “facial plausibility” when the party seeking relief “pleads
 23 factual content that allows the court to draw the reasonable inference that the defendant is liable

1 for the misconduct alleged.” *Id.* Although the Court must accept as true the Complaint’s well-
 2 pled facts, conclusory allegations of law and unwarranted inferences will not defeat an otherwise
 3 proper Fed. R. Civ. P. 12(b)(6) motion. *Vasquez v. L.A. County*, 487 F.3d 1246, 1249 (9th Cir.
 4 2007); *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). “[A] plaintiff’s
 5 obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and
 6 conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual
 7 allegations must be enough to raise a right to relief above the speculative level.” *Bell Atl. Corp.
 8 v. Twombly*, 550 U.S. 544, 555 (2007) (citations and footnote omitted). This requires a plaintiff
 9 to plead “more than an unadorned, the-defendant-unlawfully-harmed-me accusation.” *Iqbal*, 129
 10 S. Ct. at 1949 (citing *Twombly*).

11 **B. Stored Communications Act**

12 RoadLink alleges violation of the Stored Communication Act 18 U.S.C. § 2701, *et seq.*
 13 (“SCA”). The SCA creates criminal and civil liability for certain unauthorized access to stored
 14 communications and records. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir.
 15 2002). The SCA creates a private right of action against anyone who “(1) intentionally accesses
 16 without authorization a facility through which an electronic communication service is provided;
 17 or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or
 18 prevents authorized access to a wire or electric communication while it is in electronic storage in
 19 such system.” 18 U.S.C. § 2701(a)(1) and (2); *see id.* § 2707 (creating a private right of action).
 20 The SCA’s general prohibitions do not apply, however, “to conduct authorized (1) by the person
 21 or entity providing a wire or electronic communication service; [or] (2) by a user of that service
 22 with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c).

23

24

1 RoadLink asserts that Malpass violated (a)(2) when he accessed the computer provided to
 2 him by RoadLink and copied and then permanently deleted information and emails contained on
 3 the computer. Malpass urges the Court to dismiss the claim because (1) the computer system
 4 that he accessed was not a “facility” through which an electronic communication service is
 5 provided; (2) the files contained on the computer hard drive and in Microsoft Outlook were not
 6 in “electronic storage,” and; (3) even if the computer is determined to be a “facility” and the files
 7 were in “electronic storage,” RoadLink “authorized” the access. Because Malpass’s work
 8 computer was not a “facility” as defined by the SCA and because the files contained on the hard
 9 drive and Microsoft Outlook were not in “electronic storage,” RoadLink has failed to state a
 10 claim under the SCA for which relief can be granted.

11 **1. The Computer was not a Facility**

12 “To state a claim under the SCA, Plaintiff must allege that Defendant accessed without
 13 authorization ‘a facility through which an electronic communication service is provided.’ *In re*
 14 *iPhone Application Litigation*, 844 F.Supp.2d 1040, 1057 (N.D. Cal. 2012). The Act defines
 15 “electronic communication service” as “any service which provides to users thereof the ability to
 16 send and receive wire or electronic communications.” 18 U.S.C. § 2510(15). The court in *In re*
 17 *iPhone Application Litigation* granted a motion to dismiss for failure to state a claim, holding
 18 that iOS devices² were not facilities through which an electronic communication service is
 19 provided. 844 F.Supp.2d at 1057–58. The court followed the reasoning in *Crowley v.*
 20 *CyberSource Corp*, and *Chance v. Ave. A, Inc.*, which held that including a personal computing
 21 device within the definition of “facility” rendered other parts of the SCA illogical. *Id.* at 1058;
 22 166 F.Supp.2d 1263, 1271 (N.D. Cal.2001); 165 F.Supp.2d 1153, 1161 (W.D. Wash.2001). To

24 ² iOS devices (such as the iPhone, iPod, and iPad) are devices that run the iOS operating system.

1 avoid this illogical outcome, the courts have drawn a distinction between communication
 2 services providers and users. In *In re iPhone Application Litigation*, the court recognized that
 3 “the computer systems of an email provider, a bulletin board system, or an [internet service
 4 provider]” were providers, whereas the iPhone, iPod, and iPad, like a personal computer, were
 5 not. 844 F.Supp.2d at 1057–58.

6 Here, if the computer issued to Malpass was a “facility,” then any web site accessed on
 7 the computer would be a user of the communication service provided by the computer, and
 8 consequently any communication between the individual computer and the web site is a
 9 communication “of or intended for” that web site, triggering the § 2701(c)(2) exception for
 10 authorized access. Instead, Malpass and others authorized to access the computer are the user
 11 and the computer would not classify as a facility for the purposes of § 2701(a). RoadLink
 12 provides no facts to suggest that the computer was a communication service provider.

13 **2. Malpass did not Access Electronic Communications in Electronic
 Storage**

14 To state a claim under the SCA, RoadLink must show not only that Malpass accessed a
 15 facility through which an electronic communication service is provided, but furthermore that
 16 Malpass “obtained, altered, or prevented authorized access to a wire or electronic communication
 17 while it was in electronic storage in the system.” 18 U.S.C. § 2701(a). The SCA defines
 18 “electronic storage” as: (A) any temporary, intermediate storage of a wire or electronic
 19 communication incidental to the electronic transmission thereof; and (B) any storage of such
 20 communication by an electronic communication service for purposes of backup protection of such
 21 communication. 18 U.S.C. § 2510(17).

22 RoadLink alleges that Malpass destroyed and copied messages that remained on
 23 RoadLink’s server after delivery and were stored “by an electronic communication service for
 24

1 purposes of backup protection” within the meaning of subsection (B). In particular RoadLink
 2 argues that Malpass destroyed historical communications that were stored on the computer’s
 3 Microsoft Outlook program for backup purposes. However, in *Lazette v. Kulmatycki* the court
 4 dismissed the plaintiff’s SCA claim in part for failure to show that e-mails accessed by the
 5 defendant were in electronic storage. – F. Supp. 2d – (N.D. Ohio 2013), 2013 WL 2455937.
 6 Finding that, “in light of the restriction of ‘storage’ in 2510(17)(B) solely for ‘backup protection,’
 7 e-mails [that] the intended recipient has opened, but not deleted (and thus remain available for
 8 later re-opening) are not being kept ‘for backup protection.’” *Id* at 7 (citing *Jennings v. Jennings*,
 9 736 S.E.2d 242, 245 (S.C. 2012)). Following the reasoning that emails which are opened but not
 10 deleted are not in “electronic storage” for the purpose of backup protection, RoadLink has failed
 11 to assert facts that support that Malpass accessed communication in electronic storage.

12 Because RoadLink has failed to allege facts that could show that the computer hard drive
 13 was a “facility” and that the files accessed were communications in “electronic storage,” the
 14 Court does not need to address—for the purposes of the SCA claim—whether RoadLink
 15 authorized Malpass to access the information, or whether that authority terminated when he went
 16 to work for Merit. RoadLink has failed to state a claim under the SCA for which relief can be
 17 granted. Therefore, Malpass’s Motion to Dismiss RoadLink’s SCA claim is GRANTED and the
 18 claim is dismissed with prejudice.

19 **C. Computer Fraud and Abuse Act**

20 RoadLink also alleges violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030
 21 *et seq.* (“CFAA”). The CFAA was enacted in 1984 to enhance the government’s ability to
 22 prosecute computer crimes. The act was originally designed to target hackers who accessed
 23 computers to steal information or to disrupt or destroy computer functionality, as well as
 24

1 criminals who possessed the capacity to “access and control high technology processes vital to
 2 our everyday lives...” H.R. Rep. 98–894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). The
 3 CFAA prohibits a number of different computer crimes, the majority of which involve accessing
 4 computers without authorization or in excess of authorization, and then taking specified
 5 forbidden actions, ranging from obtaining information to damaging a computer or computer data.
 6 *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir.2009); See 18 U.S.C. § 1030(a)(1)-
 7 (7).

8 RoadLink alleges that Malpass violated subsections (a)(4) and (a)(5) of the CFAA. In
 9 relevant part, the CFAA prohibits:

- 10 (4) Knowingly and with intent to defraud, access[ing] a protected
 computer without authorization, or exceed[ing] authorized access,
 and by means of such conduct further[ing] the intended fraud and
 obtain[ing] anything of value, unless the object of the fraud and
 the thing obtained consists only of the use of the computer and the
 value of such use is not more than \$5,000 in any 1-year period;
- 11 (5) (A) Knowingly caus[ing] the transmission of a program,
 information, code, or command, and as a result of such conduct,
 intentionally caus[ing] damage without authorization, to a
 protected computer;
- 12 (B) Intentionally access[ing] a protected computer without
 authorization, and as a result of such conduct, recklessly caus[ing]
 damage; or
- 13 (C) Intentionally access[ing] a protected computer without
 authorization, and as a result of such conduct, caus[ing] damage
 and loss.

14 Malpass argues that RoadLink has failed to state a claim under § 1030 because (1) the
 15 computer at issue was not a “protected computer” and (2) he had authorization to access the
 16 computer and information contained within it.

1 **1. The Computer at Issue was a Protected Computer**

2 Malpass first contends that the RoadLink has failed to prove that the computer at issue
 3 was a “protected computer” under § 1030. However, the Ninth Circuit has concluded that a
 4 computer falls within the definition of a “protected computer” if it has internet access. *U.S. v.*
 5 *Nosal*, 676 F.3d 854, 859 (9th Cir.2012). RoadLink has pled facts showing that the computer at
 6 issue was able to send and receive email communication and therefore would need to have
 7 internet access. Therefore, Malpass’s argument that the computer at issue is not a “protected
 8 computer” is without merit.

9 **2. RoadLink Granted Malpass Authorization to Access the Computer and the
 10 Information**

11 Malpass also argues that RoadLink’s CFAA claims are deficient because Malpass was
 12 given authorization for unlimited access to the computer and files at issue. The Ninth Circuit has
 13 determined that “an employer gives an employee ‘authorization’ to access a company computer
 14 when the employer gives the employee permission to use it.” *LVRC Holdings LLC*, 581 F.3d at
 15 1133. A person who “exceeds authorized access” “has permission to access the computer, but
 16 accesses information on the computer that the person is not entitled to access. *Id.*; see 18 U.S.C.
 17 § 1030(e)(6).

18 In *Nosal*, the Ninth Circuit held that the CFAA is concerned only with unauthorized
 19 access of information, not its unauthorized use. *U.S. v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012).
 20 There, employees at an executive search firm sent documents from a confidential company
 21 database to which they had access to a former employee who had started a competing company.
 22 *Id.* at 856. The Ninth Circuit dismissed the charges of a CFAA violation, holding that the “plain
 23 language of the CFAA targets the unauthorized procurement or alteration of information, not its
 24 misuse or misappropriation.” *Id.* at 863.

1 Here, RoadLink granted Malpass authorization to access the information on the computer
 2 he is alleged to have copied and deleted. (Dkt. #1, Compl. at ¶15). RoadLink gave Malpass a
 3 computer with which he could maintain and update the Trade Resources and other files. *Id.*
 4 Under the Ninth Circuit's interpretation of the CFAA, Malpass's alleged subsequent actions—
 5 copying and deleting the files in the database—do not implicate the CFAA. These alleged
 6 actions concern the "misuse or misappropriation" of the Trade Resources, something the CFAA
 7 does not target. Therefore, Malpass did not "exceed authorized access" under the CFAA, and
 8 RoadLink has failed to state a claim under the CFAA for which relief can be granted. Malpass's
 9 Motion to Dismiss RoadLink's CFAA claim is GRANTED and the claim is dismissed with
 10 prejudice.

11 **D. Jurisdiction**

12 Malpass argues that, because the only two federal claims have been dismissed and the
 13 remaining claims are state claims, the Court should dismiss the remaining claims for lack of
 14 subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). This argument fails for two reasons. First,
 15 the dismissal of the federal claims does not deprive the Court of subject matter jurisdiction. All
 16 of RoadLink's claims are part of the same case or controversy. Thus, the Court had subject
 17 matter jurisdiction over *all* claims when the complaint was filed alleging claims under the two
 18 federal acts. 28 U.S.C. §§ 1331, 1337. The Court does not lose subject matter jurisdiction over
 19 the state claims when a plaintiff asserting a federal claim does not prevail on that claim. 28
 20 U.S.C. § 1337. Instead, the Court retains supplemental jurisdiction over the claims unless it
 21 declines to exercise jurisdiction for reasons such as judicial economy, convenience, fairness, and
 22 comity. *Sanford v. MemberWorks, Inc.*, 625 F.3d 550, 561 (9th Cir. 2005). The Court has not
 23 declined to exercise jurisdiction here.

1 Furthermore, and in any event, the Court has diversity jurisdiction over the remaining
2 claims. 28 U.S.C. § 1332(a). The parties are completely diverse, and RoadLink’s complaint
3 states plainly that “the amount in controversy exceeds \$75,000.” (Dkt. #1, Compl. at ¶ 5).
4 Malpass has provided no facts to show that this amount is listed in bad faith or that there is a
5 legal certainty that the claims are really for less than \$75,000. *Budget Rent-A-Car, Inc.* v.
6 *Higashiguchi*, 109 F.3d 1471, 1473 (9th Cir. 1997) (To justify dismissal, “it must appear to a
7 legal certainty that the claim is really for less than the jurisdictional amount.”). Therefore,
8 Malpass’s argument fails and the Court retains jurisdiction over the remaining claims.

III. Conclusion

10 Malpass's Motion to Dismiss the Stored Communication Act claims and the Computer
11 Fraud and Abuse Act claims is **GRANTED**. Malpass's Motion to Dismiss the remaining claims
12 for lack of subject matter jurisdiction is **DENIED**.

13 || IT IS SO ORDERED.

14 Dated this 18th day of September, 2013.

Ronald B. Leighton
RONALD B. LEIGTON
UNITED STATES DISTRICT JUDGE